杀毒软件终结者病毒

杀毒软件终结者是最近危害比较大的一个病毒。该病毒利用了 IFEO 重定向劫持技术,会使大量的杀

毒软件和安全相关工具无法运行；会破坏安全模式，使中毒用户无法在安全模式下查杀病毒；会下载

大量病毒到用户计算机来盗取用户有价值的信息和某些帐号；能通过可移动存储介质传播。

病毒的详细信息如下：

1、在系统中生成病毒文件，包括：

C:Program FilesCommon FilesMicrosoft SharedMSInfo{随机 8 位字母+数字名字}.dat

C:Program FilesCommon FilesMicrosoft SharedMSInfo{随机 8 位字母+数字名字}.dll

%windir%{随机 8 位字母+数字名字}.hlp

%windir%Help{随机 8 位字母+数字名字}.chm

也有可能生成如下文件

%sys32dir%{随机字母}.exe

替换%sys32dir%verclsid.exe 文件

2、生成以下注册表项将病毒已动态库文件的形式插入到系统进程中运行

HKEY_CLASSES_ROOTCLSID'随机 CLSID'InprocServer32 '病毒文件全路径'

HKEY_LOCAL_MACHINESOFTWAREClassesCLSID'随机 CLSID' '病毒文件全路径'

HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionExplorerShellExecuteHooks

'生成的随机 CLSID'

HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun

'随机字符串' '病毒文件全路径'

3、监视并关闭以下进程以及窗口

AntiVirus

TrojanFirewall

Kaspersky

JiangMin

KV200

kxp

Rising

RAV

RFW

KAV200

KAV6

McAfe

Network Associates

TrustPort

NortonSymantec

SYMANT~1

Norton SystemWorks

ESET

Grisoft

F-Pro

Alwil Software

ALWILS~1

F-Secure

ArcaBit

Softwin

ClamWin

DrWe

Fortineanda Software

Vba3

Trend Micro

QUICKH~1

TRENDM~1

Quick Heal

eSafewido

Prevx1

ers

avg

Ikarus

SophoSunbeltPC-cilli

ZoneAlar

Agnitum

WinAntiVirus

AhnLab

Normasurfsecret

BullguardBlac

360safe

SkyNet

Micropoint

Iparmor

ftc

mmjk2007

Antiy Labs

LinDirMicro Lab

Filseclab

ast

System Safety Monitor

ProcessGuard

FengYun

Lavasoft

NOD3

mmsk

The Cleaner

Defendio

kis6Beheadsreng

IceSword

HijackThis

killbox

procexp

Magicset

EQSysSecureProSecurity

Yahoo!

Google

baidu

P4P

Sogou PXP

ardsys

超级兔子木马

KSysFiltsys

KSysCallsys

AVK

K7

Zondex

blcorp

Tiny Firewall Pro

Jetico

HAURI

CA

kmx

PCClear_Plus

Novatix

Ashampoo

WinPatrol

Spy Cleaner Gold

CounterSpy

EagleEyeOS

Webroot

BufferZ

avp

AgentSvr

CCenter

Rav

RavMonD

RavStub

RavTask

rfwcfg

rfwsrv

RsAgent

Rsaupd

runiep

SmartUp

FileDsty

RegClean

360tray

360Safe

360rpt

kabaload

safelive

Ras

KASMain

KASTask

KAV32

KAVDX

KAVStart

KISLnchr

KMailMon

KMFilter

KPFW32

KPFW32X

KPFWSvc

KWatch9x

KWatch

KWatchX

TrojanDetector

UpLive.EXE

KVSrvXP

KvDetect

KRegEx

kvol

kvolself

kvupload

kvwsc

UIHost

IceSword

iparmo

mmsk

adam

MagicSet

PFWLiveUpdate

SREng

WoptiClean

scan32

hcfg32

mcconsol

HijackThis

mmqczj

Trojanwall

FTCleanerShell

loaddll

rfwProxy

KsLoader

KvfwMcl

autoruns

AppSvc32

ccSvcHst

isPwdSvc

symlcsvcnod32kui

avgrssvc

RfwMain

KAVPFW

Iparmor

nod32krn

PFW

RavMon

KAVSetup

NAVSetup

SysSafe

QHSET

zxsweep.

AvMonitor

UmxCfg

UmxFwHlp

UmxPol

UmxAgent

UmxAttachment

KPFW32

KPFW32X

KvXP_1

KVMonXP_1

KvReport

KVScan

KVStub

KvXP

KVMonXP

KVCenter

TrojDie

avp.com.

krepair.COM

KaScrScn.SCR

Trojan

Virus

kaspersky

jiangmin

rising

ikaka

duba

kingsoft

360safe

木马

病毒

杀毒

查毒

防毒

反病毒

专杀

卡巴斯基

江民

瑞星

卡卡社区

金山毒霸

毒霸

金山社区

360 安全

恶意软件

流氓软件

4、生成以下注册表项来进行文件映像劫持(IFEO 劫持)，使用户运行文件名映像被劫持的文件时先

运行病毒文件，从而阻止相关安全软件运行。

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Options360rpt.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Options360Safe.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Options360tray.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Optionsadam.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsAgentSvr.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsAppSvc32.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Optionsautoruns.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Optionsavgrssvc.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsAvMonitor.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Optionsavp.com

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Optionsavp.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsCCenter.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsccSvcHst.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsFileDsty.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Options

FTCleanerShell.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Options

HijackThis.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsIceSword.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Optionsiparmo.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsIparmor.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsisPwdSvc.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Optionskabaload.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKaScrScn.SCR

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKASMain.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKASTask.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKAV32.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKAVDX.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKAVPFW.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKAVSetup.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKAVStart.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKISLnchr.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKMailMon.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKMFilter.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKPFW32.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKPFW32X.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKPFWSvc.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKRegEx.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Optionskrepair.COM

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKsLoader.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKVCenter.kxp

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKvDetect.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKvfwMcl.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKVMonXP.kxp

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKVMonXP_1.kxp

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Optionskvol.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Optionskvolself.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKvReport.kxp

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKVScan.kxp

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKVSrvXP.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKVStub.kxp

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Optionskvupload.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Optionskvwsc.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKvXP.kxp

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKvXP_1.kxp

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKWatch.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKWatch9x.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsKWatchX.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Optionsloaddll.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsMagicSet.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Optionsmcconsol.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Optionsmmqczj.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Optionsmmsk.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsNAVSetup.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Optionsnod32krn.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Optionsnod32kui.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsPFW.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution Options

PFWLiveUpdate.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File Execution OptionsQHSET.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution OptionsRas.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution OptionsRav.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution OptionsRavMon.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution OptionsRavMonD.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution OptionsRavStub.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution OptionsRavTask.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution OptionsRegClean.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution Optionsrfwcfg.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution OptionsRfwMain.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution OptionsrfwProxy.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution Optionsrfwsrv.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution OptionsRsAgent.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution OptionsRsaupd.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution Optionsruniep.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution Optionssafelive.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution Optionsscan32.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution Optionsshcfg32.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution OptionsSmartUp.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution OptionsSREng.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution Options

symlcsvc.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution OptionsSysSafe.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution Options

TrojanDetector.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution Options

Trojanwall.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution OptionsTrojDie.kxp

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution OptionsUIHost.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution OptionsUmxAgent.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution Options

UmxAttachment.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution OptionsUmxCfg.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution OptionsUmxFwHlp.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution OptionsUmxPol.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution OptionsUpLive.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution Options

WoptiClean.exe

HKLMSOFTWAREMicrosoftWindows NTCurrentVersionImage File

Execution Optionszxsweep.exe

上述文件都被劫持到 C:Program FilesCommon FilesMicrosoft

SharedMSInfo 下面的那个 dat 文件

5、修改以下注册表，导致无法显示隐藏文件

HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionExplor

erAdvancedHidden

dword:00000002

HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionEx

plorerAdvancedFolderHidden

SHOWALL CheckedValue

dword:00000000

6、修改以下服务的启动类型来禁止 Windows 的自更新和系统自带的防火墙

HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesSharedAccess

Start dword:00000004

HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServiceswuauserv

Start dword:00000004

7、删除以下注册表项，使用户无法进入安全模式 PPServer

HKEY_CURRENT_USERSYSTEMCurrentControlSetControlSafeBootMinim

al

{4D36E967-E325-11CE-BFC1-08002BE10318}

HKEY_CURRENT_USERSYSTEMControlSet001ControlSafeBootMinimal

{4D36E967-E325-11CE-BFC1-08002BE10318}

8、修改常见杀毒软件服务的 start 键值为 0x00000004

HKLMSYSTEMControlSet001ServicesRfwServiceStart: 0x00000004

9、修改注册表，关闭系统自动更新

修改 HKLMSYSTEMCurrentControlSetServiceswuauservStart

和 HKLMSYSTEMCurrentControlSetServiceswscsvcstart

的键值为 0x00000004

10、连接网络下载病毒，包括自身的病毒更新和其他一些木马程序（ARP 木马）

11、关闭杀毒软件实时监控窗口，如瑞星、卡巴，通过自动点击'跳过'按钮来逃过查杀

12、禁止用户通过浏览器访问包含特殊字符串（如：病毒）的网页。

13、在硬盘分区生成文件：autorun.inf 和 随机字母+数字组成的病毒复制体，并修改

“NoDriveTypeAutoRun”使病毒可以随可移动存储介质传播。

解决办法：

由于该病毒的特殊性，一旦用户感染后即使是格式化系统盘后重新安装系统也可能会被系统中其他

分区中的病毒感染，因此不建议使用手动查杀。各杀毒厂商都已经提供了相应的专杀工具，你可以

到各厂商的官方网站下载。

瑞星专杀工具 http://download.rising.com.cn/zsgj/orangeaug.com

金山专杀工

具 http://down.www.kingsoft.com/db/download/othertools/DubaTool_AV_Killer2.COM

需要提醒用户的是由于该病毒还会下载其他木马病毒运行，因此在使用专杀后您还需要使用杀毒软

件进行全盘扫描。